AO 106 (Rev. 04/10) Application for a Search Warrant

HH/EC

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Residence located at 159 W. 6th Avenue Lancaster, OH 43130, including any curtilage, detached buildings and any person or digital device located therein

Case No. 2:21-mj-76

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A, incorporated herein by this reference.

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized):*

See Attachment B, incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC Sec 2251	Advertising of/for child pornography/visual depictions of minors engaged in sexually explicit conduct
18 USC Secs 2252 and 2252A	Receipt/possession/distribution of child pornography/visual depictions of minors engaged in sexually explicit conduct

The application is based on these facts:

See attached affidavit, incorporated herein by this reference.

☑ Continued on the attached sheet.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Brett M. [illegible], FBI TFO

Printed name and title

Sworn to before me and signed in my presence.

Date: 2-3-21

Judge's signature

City and state: Columbus, Ohio

Chelsey M. Vascura, U.S. Magistrate Judge

Printed name and title

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT
EASTERN DIVISION OF OHIO

In the Matter of the Search of:	)	**No.**
	)	
The residence located at	)	**Magistrate Judge**
159 W. 6th Avenue Lancaster, OH 43130	)	
including any curtilage, detached buildings and	)	
any person or digital device located therein	)	

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Brett M. Peachey, a Task Force Officer with the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state:

I. EDUCATION, TRAINING, AND EXPERIENCE

1. I, TFO Brett M. Peachey, have been employed as a police officer with the City of Westerville since December of 1995. In March of 2008, I began as a Task Force Officer for the FBI, and am currently assigned to the Child Exploitation and Human Trafficking Task Force, Cincinnati Division, Columbus Resident Agency. I am primarily responsible for investigating internet crimes against children, including child pornography offenses and the online exploitation of children.
2. During my career as a Criminal Investigator and TFO, I have participated in various investigations of computer-related offenses and have executed numerous search warrants, including those involving searches and seizures of computers, computer equipment, software, and electronically stored information. I have received both formal and informal training in the detection and investigation of computer-related offenses. As part of my duties as a Criminal Investigator and task force officer, I investigate criminal violations relating to child exploitation and child pornography including the online enticement of minors and the illegal distribution, transmission, receipt, possession, and production of child pornography, in violation of 18 U.S.C. §§ 2252, 2252A, 2251 and 2422.

II. PURPOSE OF THE AFFIDAVIT

3. The facts and statements set forth in this affidavit are based on my knowledge, experience, and investigation, as well as the knowledge, experience, and investigative findings of

others with whom I have had communications about this investigation, including other law enforcement officers and agents. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts I believe are necessary to establish probable cause for a warrant to search the residence located at 159 W. 6th Avenue Lancaster, OH 43130 (the SUBJECT PREMISES) pursuant to Rule 41 of the Federal Rules of Criminal Procedure.

4. The SUBJECT PREMISES to be searched is more particularly described in Attachment A, for the items specified in Attachment B, which items constitute instrumentalities, fruits, and evidence of violations of 18 U.S.C. §§ 2251, 2252, and 2252A, – the advertising of/for, distribution, transmission, receipt, and/or possession of child pornography. I am requesting authority to search the entire SUBJECT PREMISES, including the residential dwelling, curtilage, including detached buildings and storage units, any individual located therein that may have any mobile computing devices concealed on their person, and any computer and/or digital media located therein/thereon, for evidence, fruits, and instrumentalities of the above violations.

III. APPLICABLE STATUTES AND DEFINITIONS

5. Title 18 United States Code, Section 2251(d)(1)(A) makes it a federal crime for any person to make, print, publish, or cause to be made, printed or published, any notice or advertisement that seeks or offers to receive, exchange, buy, produce, display, distribute or reproduce, any visual depiction involving the use of a minor engaging in sexually explicit conduct, if such person knows or has reason to know that either the notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail; or that the notice or advertisement actually was transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce, including by computer or mail.

6. Title 18, United States Code, Section 2252, makes it a federal crime for any person to knowingly transport, receive, distribute, possess or access with intent to view any visual depiction of a minor engaging in sexually explicit conduct, if such receipt, distribution or possession utilized a means or facility of interstate commerce, or if such visual depiction has been mailed, shipped or transported in or affecting interstate or foreign commerce.

This section also prohibits reproduction for distribution of any visual depiction of a minor engaging in sexually explicit conduct, if such reproduction utilizes any means or facility of interstate or foreign commerce, or is in or affecting interstate commerce.

7. Title 18, United States Code, Section 2252A, makes it a federal crime for any person to knowingly transport, receive or distribute any child pornography using any means or facility of interstate commerce, or any child pornography that has been mailed, or any child pornography that has shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. This section also makes it a federal crime to possess or access with intent to view any material that contains an image of child pornography that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce, or in or affecting interstate commerce by any means, including by computer.

8. As it is used in 18 U.S.C. §§ 2251 and 2252, the term "sexually explicit conduct" is defined in 18 U.S.C. § 2256(2)(A) as actual or simulated: sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic area of any person.

9. As it is used in 18 U.S.C. § 2252A(a)(2), the term "child pornography"[1] is defined in 18 U.S.C. § 2256(8) as: any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: (A) the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; (B) such visual depiction is a digital image, computer image, or computer generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or (C) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

10. The term "sexually explicit conduct" has the same meaning in § 2252A as in § 2252, except that for the definition of child pornography contained in § 2256(8)(B), "sexually explicit conduct" also has the meaning contained in § 2256(2)(B): (a) graphic sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether

1 The term child pornography is used throughout this affidavit. All references to this term in this affidavit include both visual depictions of minors engaged in sexually explicit conduct as referenced in 18 U.S.C. §

between persons of the same or opposite sex, or lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited; (b) graphic or lascivious simulated (i) bestiality, (ii) masturbation, or (iii) sadistic or masochistic abuse; or (c) graphic or simulated lascivious exhibition of the genitals or pubic area of any person.

11. The term "minor", as used herein, is defined pursuant to Title 18, United States Code, Section 2256(1) as "any person under the age of eighteen years."

12. The term "graphic," as used in the definition of sexually explicit conduct contained in 18 U.S.C. § 2256(2)(B), is defined pursuant to 18 U.S.C. § 2256(10) to mean "that a viewer can observe any part of the genitals or pubic area of any depicted person or animal during any part of the time that the sexually explicit conduct is being depicted."

13. The term "visual depiction," as used herein, is defined pursuant to T18 U.S.C. § 2256(5) to "include undeveloped film and videotape, and data stored on computer disk or by electronic means which is capable of conversion into a visual image."

14. The term "computer"[2] is defined in 18 U.S.C. § 1030(e)(1) as an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device.

15. "Cellular telephone" or "cell phone" means a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books"; sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving videos; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may

---

2252 and child pornography as defined in 18 U.S.C. § 2256(8).

2 The term computer is used throughout this Affidavit and in the Attachments hereto to refer not only to traditional desktop and laptop computers, but also other mobile devices such as cellular phones, tablets and digital storage media. Where the capabilities of these devices differ significantly from that of traditional computers, those capabilities are

include geographic information indicating where the cell phone was at particular times.

IV. BACKGROUND REGARDING THE INTERNET AND MOBILE APPLICATIONS

16. I know from my training and experience that computer hardware, mobile computing devices, computer software, and electronic files ("objects") may be important to criminal investigations in two distinct ways: (1) the objects themselves may be evidence, instrumentalities, or fruits of crime, and/or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data. Rule 41 of the Federal Rules of Criminal Procedure permits the government to search for and seize computer hardware, software, and electronic files that are evidence of a crime, contraband, and instrumentalities and/or fruits of crime.

17. Computers, mobile devices and the Internet have revolutionized the ways in which those with a sexual interest in children interact with each other and with children they seek to exploit. These new technologies have provided ever-changing methods for exchanging child pornography and communicating with minors. Digital technology and the Internet serve four functions in connection with child pornography and child exploitation: production, communication, distribution, and storage.

18. Computers, tablets and smart/cellular phones ("digital devices") are capable of storing and displaying photographs. The creation of computerized or digital photographs can be accomplished with several methods, including using a "scanner," which is an optical device that can digitize a photograph. Another method is to simply take a photograph using a digital camera or cellular phone with an onboard digital camera, which is very similar to a regular camera except that it captures the image in a computerized format instead of onto film. Such computerized photograph files, or image files, can be known by several file names including AGIF@ (Graphic Interchange Format) files, or "JPG/JPEG" (Joint Photographic Experts Group) files.

19. Digital devices are also capable of storing and displaying movies of varying lengths. The creation of digital movies can be accomplished with several methods, including using a digital video camera (which is very similar to a regular video camera except that it captures the image in a digital format which can be transferred onto the computer). Such

---

explained separately.

computerized movie files, or video files, can be known by several file names including "MPG/MPEG" (Moving Pictures Experts Group) files.

20. The capability of digital devices to store images in digital form makes them an ideal repository for child pornography. A single CD, DVD, or USB thumb drive can store hundreds or thousands of image files and videos. It is not unusual to come across USB thumb drives that are as large as 128GB. The size of hard drives and other storage media that are used in home computers and cellular phones have grown tremendously within the last several years. Hard drives with the capacity of several terabytes are not uncommon. These drives can store hundreds of thousands of images and videos at very high resolution. Tablet devices have average storage capabilities ranging from 16 Gigabytes to 256 Gigabytes. In addition, most tablets have the ability to utilize the various drives (thumb, jump or flash) described above, which can allow a user to access up to an additional 256 Gigabytes of stored data via the tablet. Modern cell phones have average storage capabilities ranging from 4 Gigabytes to 128 Gigabytes. In addition, most cellular phones have the ability to utilize micro SD cards, which can add up to an additional 128 Gigabytes of storage. Media storage devices and cellular phones can easily be concealed and carried on an individual's person. Mobile computing devices, like cellular phones and tablets, also have the ability to take still and moving images that are easily stored, manipulated or transferred between devices using software or applications installed on each device. Additionally, multiple devices can be synced to a single account and when an image or video file is transferred it can be transferred to all devices synced to the account at the same time. As a result of this technology, it is relatively inexpensive and technically easy to produce, store and distribute child pornography. Magnetic storage located in host computers adds another dimension to the equation. It is possible to use a video camera to capture an image, process that image in a computer with a video capture board, and to save that image by storing it in another country. Once this is done, there is no readily apparent evidence at the scene of the crime. Only with careful laboratory examination of electronic storage devices is it possible to recreate the evidence trail.

21. The Internet is a worldwide network of computer systems operated by governmental entities, corporations, and universities. With a computer or mobile device connected to the Internet, an individual user can make electronic contact with millions of other computer or mobile device users around the world. Many individual computer/mobile device users and

businesses obtain their access to the Internet through businesses known as Internet Service Providers ("ISPs"). ISPs provide their customers with access to the Internet using wired telecommunications lines, wireless signals commonly known as Wi-Fi, and/or cellular service; provide Internet e-mail accounts that allow users to communicate with other Internet users by sending and receiving electronic messages through the ISPs' servers or cellular network; remotely store electronic files on their customers' behalf; and may provide other services unique to each particular ISP. ISPs maintain records pertaining to the individuals or companies that have subscriber accounts with the ISP. Those records may include identifying and billing information, account access information in the form of log files, e-mail transaction information, posting information, account application information, Internet Protocol ("IP") addresses and other information both in computer data format and in written record format.

22. These internet-based communication structures are ideal for those seeking to find others who share a sexual interest in children and child pornography, or seeking to exploit children online. Having both open as well as anonymous communication capability allows the user to locate others of similar inclination and still maintain their anonymity. Once contact has been established, it is then possible to send messages and graphic images to other trusted child pornography collectors or to vulnerable children who may not be aware of the user's true identity. Moreover, the child pornography collector need not use large service providers. Child pornography collectors can use standard Internet connections, such as those provided by businesses, universities, and government agencies, to communicate with each other or with children, and to exchange child pornography. These communication links allow contacts around the world as easily as calling next door. Additionally, these communications can be quick, relatively secure, and as anonymous as desired.

23. It is often possible to recover digital or electronic files, or remnants of such files, months or sometimes even years after they have been downloaded onto a hard drive or other digital device, deleted, or viewed via the Internet. Such files can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or even years later using readily available forensic tools. When a person "deletes" a file from a digital device, the data contained in the files does not actually disappear; rather the data remains on the device until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space - that is, space on a storage medium that

is not allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

24. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve residue of an electronic file from a hard drive depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer habits.

25. As is the case with most digital technology, communications by way of computer or mobile devices can be saved or stored on the computer or mobile device used for these purposes. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or mobile device, or saving the location of one's favorite websites in, for example, "bookmarked" files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically stored in many places, such as temporary files or ISP client software, among others. In addition to electronic communications, a computer user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

26. Searching computer systems and electronic storage devices may require a range of data analysis techniques. Criminals can mislabel or hide files and directories, encode communications, attempt to delete files to evade detection, or take other steps to frustrate law enforcement searches. In light of these difficulties, your affiant requests permission to use whatever data analysis techniques appear necessary to locate and retrieve the evidence described in Attachment B.

27. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications. Mobile applications, also referred to as "apps," are small, specialized programs downloaded onto mobile devices that enable users to perform a variety of functions, including engaging in online chat, reading a book, or playing a game. Examples of such "apps" include LiveMe, KIK messenger service, Snapchat, Meet24, and Instagram. Kik is a free mobile application that can be downloaded on Android or iOS devices that permits users to communicate anonymously with fellow Kik users. This

application allows users to create groups where like-minded individuals can chat/text other users and post videos/images which includes groups in the sexual exploitation of children. Kik allows users to create a unique username for each individual's account, but each user also has the ability to create a screen name that the user can change at any time.

V. SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS

28. Searches and seizures of evidence from computers, mobile computing devices, and external storage media commonly require agents to download or copy information from the computers and their components, or seize most or all computer items (computer hardware, computer software, and computer related documentation) to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following:

    a. Computer storage devices (like hard disks, diskettes, tapes, laser disks, magneto opticals, and others) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data to determine whether it is included in the warrant. This sorting process can take days or weeks, depending on the volume of data stored, and it would be generally impossible to accomplish this kind of data search on site; and

    b. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure which is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

29. In order to fully retrieve data from a computer system, the analyst needs all magnetic storage devices as well as the central processing unit (CPU). In cases involving child

pornography where the evidence consists partly of graphics files, the monitor(s) may be essential for a thorough and efficient search due to software and hardware configuration issues. In addition, the analyst needs all the system software (operating systems or interfaces, and hardware drivers) and any applications software, which may have been used to create the data (whether stored on hard drives or on external media).

30. In addition, there is probable cause to believe that any computer or mobile computing device and its storage devices, the monitor, keyboard, and modem are all instrumentalities of the crime(s), within the meaning of 18 U.S.C. §§ 2251, 2252, and 2252A and should all be seized as such.

VI. SEARCH METHODOLOGY TO BE EMPLOYED

31. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. Examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth in Attachment B;

b. Searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth in Attachment B;

c. Surveying various files, directories and the individual files they contain;

d. Opening files in order to determine their contents;

e. Scanning storage areas;

f. Performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment B; and/or

g. Performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

VII. INVESTIGATION AND PROBABLE CAUSE

32. On April 18, 2020, TFO Kurt Jemmett of the Salt Lake City Police Department was conducting online investigations into subjects involved in the sexual exploitation of

children. Jemmett was posing as a 13-year-old female and had created fictitious profiles of this female persona on several social media platforms. On this date, Jemmett was utilizing the Kik messaging app and was contacted by a subject utilizing the Kik username "mater1239" and screen name of "DaddyMater" who was later positively identified as Trevor Beck. During the conversation, Beck solicited Jemmett's persona to engage in oral sex and, after Jemmett reminded Beck that the persona was 13 years old, Beck responded "what if I tell you I love teen pussy." Beck then sent a photo of himself and advised that he lived in Ohio.

33. As the conversation continued, Beck proceeded to send 18 videos and 12 images to Jemmett that depicted males and females of various ages nude and/or engaged in sexual activity or masturbation. Although the ages of some of the children in the files were difficult to determine and some showed signs of puberty, other files clearly depicted prepubescent children. Below is a description of some of the files Beck distributed to Jemmett during their conversation:

- A 53-second video depicting a prepubescent female, approximately 12 years of age, nude from the waist down. The female proceeds to lift her leg and spread her buttocks clearly exposing her vagina and anus on several occasions.
- A 22-second video depicting a female approximately 13 to 15 years of age. A male is masturbating and ejaculates on her face and she then proceeds to perform oral sex on the male.
- A one minute and 55-second video depicting a female, approximately 14 to 15 years of age, nude from the waist down and her breasts exposed. The female has very little breast development and a dog performs oral sex on her.
- A 24-second video depicting a female, approximately 12 years of age with slight breast development, nude from the waist up. The female proceeds to apply wooden clothes pins on each of her nipples.
- A one minute and five second video depicting two nude females, approximately 11 to 14 years of age, in which one of the females is performing oral sex on the other.
- Three videos depicting a male and female, approximately 11 to 13 years of age. The female is clothed but proceeds to expose her breasts. The male is nude and a dog appears to perform oral sex on him in the background for a short period of time. In the third video, the female briefly masturbates the male.

It should also be noted that, during the conversations, Beck repeatedly requested that Jemmett send photos of the juvenile persona's breasts.

34. A subpoena was served on Kik requesting subscriber information, including any IP address logins, for the Kik username "mater1239." Kik responded with the following information:

First Name:	Daddy-Mater
Last Name:	(not buying)
Email:	tbeck1239@gmail.com

Kik also provided information pertaining to dozens of logins for the mater1239 account between April 14th and May 14th, 2020, in which the account was accessed utilizing IP address 75.187.98.157.

35. IP address 75.187.98.157 is owned by Charter Communications. On May 14, 2020, a subpoena was served on Charter Communications requesting subscriber information for this IP address on one of the dates that this IP address was utilized to access the "mater1239" Kik account. On May 18, 2020, Charter responded with the following subscriber information:

Name:	Trevor Beck
Address:	159 W. 6th Avenue Lancaster, OH 43130
Phone:	740-785-9576

36. A search of the Ohio Law Enforcement Gateway (OHLEG) revealed that Trevor Beck has a valid driver's license registered to him at 159 W. Sixth Avenue Lancaster, OH 43130. In addition, a comparison of Beck's driver's license photo revealed that he is the same person depicted in the photo that was sent to Jemmett during their Kik conversation.

37. On September 23, 2020, an FBI agent working undercover in the Louisville, Kentucky Field Office was conducting undercover investigations involving subjects involved in the online sexual exploitation of children. The undercover entered a Kik group chat titled #tab.oochat2" when he observed another Kik user utilizing the screen name "Mater" distributing videos of child pornography. According to the undercover agent's report, he observed "Mater" distribute the following videos in the group chat for members to view:

- One video depicting a prepubescent female lying on her back wearing a blue shirt. Pens are inserted into her anus and vagina and she proceeds to masturbate.

- One video depicting a female with slight breast development in engaged in sexual intercourse with a dog.
- One video depicting an age indeterminate female digitally stimulating a penis until the male ejaculates on her.
- One video depicting a female, age approximately 15 to 16 years old, laying on her back nude. The camera pans to her genital area.
- One video depicting a female with no pubic hair laying on her back. She is engaged in sexual intercourse with a dog.
- One video depicting a prepubescent female performing oral sex on a dog. This child has previously been identified by the National Center for Missing and Exploited Children as a child victim.
- One video depicting a minor female masturbating using a foreign object placed in her vagina.

The undercover agent was able to preserve the videos that were posted in the room using screen shots and screen recordings.

38. The undercover agent was able to observe the Kik account utilizing the screen name "Mater" was assigned the username "therealmater1239." A subpoena was served on Kik requesting subscriber information, including any IP address logins, for the username "therealmater1239." Kik responded with the following information:

First Name: Mater
Last Name: (New Account)
Email: theangryleprechaun@gmail.com

Kik also provided information pertaining to dozens of logins for the "therealmater1239" account between September 7th and October 7th, 2020, in which the account was accessed utilizing IP address 75.187.98.157 for the majority of access events. This is the same IP address that was utilized by the "mater1239" Kik account that communicated with SA Jemmett. After learning of the ongoing investigation of Beck at this IP address by the Salt Lake City Division, no other follow-up was done by the Louisville Division, and the information pertaining to the investigation was forwarded to your affiant.

39. After receiving the leads from the Salt Lake City and Louisville Field Offices regarding Beck, your affiant, acting in an undercover capacity, contacted Beck at the Kik username

"therealmater1239" on November 30, 2020. Beck responded and, after a few messages, stated "I like beast [bestiality] play" and asked "You have any kids?" Your affiant, who utilizes an online undercover persona of a mother with two children responded that he did. Beck soon advised that he lived in central Ohio and asked "How old are your daughters" to which your affiant replied that they were ten and three years of age. After several other messages Beck asked "So have you played with your daughters at all?" and then inquired if he and your affiant's persona could engage in sexual intercourse in front of the children. After requesting one, your affiant received a photo which matched Beck's current Ohio driver's license photo. When asked what his darkest fantasy was, Beck responded "My top 2 are incest and teen girls. But I want to have my own daughter to have sex with and have an open nudist family." Beck then asked your affiant "would you train your daughters to take a knot" which refers to engaging in bestiality.

40. On December 30, 2020 and January 11, 2021, investigators have observed a 1994 Ford Thunderbird with Ohio registration CTFXC09 parked on the street in the area of the SUBJECT PREMISES, which is registered to Trevor Beck at that address.

VIII. COMMON CHARACTERISTICS OF INDIVIDUALS WITH A SEXUAL INTEREST IN CHILDREN

41. Based on my own knowledge, experience, and training in child exploitation and child pornography investigations, and the training and experience of other law enforcement officers with whom I have had discussions, there are certain characteristics common to individuals involved in communicating about and engaging in sexual abuse of children

A. Those who communicate about and engage in sexual abuse of children and exchange or collect child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature and communications about such activity.

B. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, video tapes,

books, slides and/or drawings or other visual media, including digital files. Child pornography collectors oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

C. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography sometimes maintain any "hard copies" of child pornographic material that may exist that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. These child pornography collections and communications are often maintained for several years and are kept close by, usually at the collector's residence. In some recent cases, however, some people who have a sexual interest in children have been found to download, view, then delete child pornography on a cyclical and repetitive basis, and to regularly delete any communications about the sexual abuse of children rather than storing such evidence on their computers or digital devices. Traces of such activity can often be found on such people's computers or digital devices, for months or even years after any downloaded files have been deleted.

D. Those who communicate about and engage in sexual abuse of children and trade or collect child pornography also may correspond with and/or meet others to share information and materials; rarely destroy correspondence from other child pornography distributors/collectors; conceal such correspondence as they do their sexually explicit material; and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

E. When images and videos of child pornography or communications about sexual abuse of children are stored on computers and related digital media, forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years even after such images and

videos have been deleted from the computers or digital media.

42. Based upon the conduct of individuals involved in trafficking in child pornography set forth in the above paragraphs, namely, that they tend to maintain their collections at a secure, private location for long periods of time, and that forensic evidence of the downloading, saving, and storage of such evidence may remain on the computers or digital media for months or even years after such evidence has been deleted from the computers or digital media, there is probable cause to believe that evidence of the offenses of receiving, distributing and possessing child pornography is currently located at the SUBJECT PREMISES, and will be recovered during forensic examination of any devices found within the SUBJECT PREMISES or on individuals located in the SUBJECT PREMISES.

IX. CONCLUSION

43. Based on the aforementioned factual information, your affiant submits there is probable cause to believe that violations of Title 18, United States Code, Sections 2251, 2252, and 2252A have been committed, and evidence of those violations is located in the residence described in Attachment A. Your affiant respectfully requests that the Court issue a search warrant authorizing the search and seizure of the items described in Attachment B.

Brett M. Peachey
Task Force Officer
Federal Bureau of Investigation

Sworn to and subscribed before me this 3 day of February 2021.

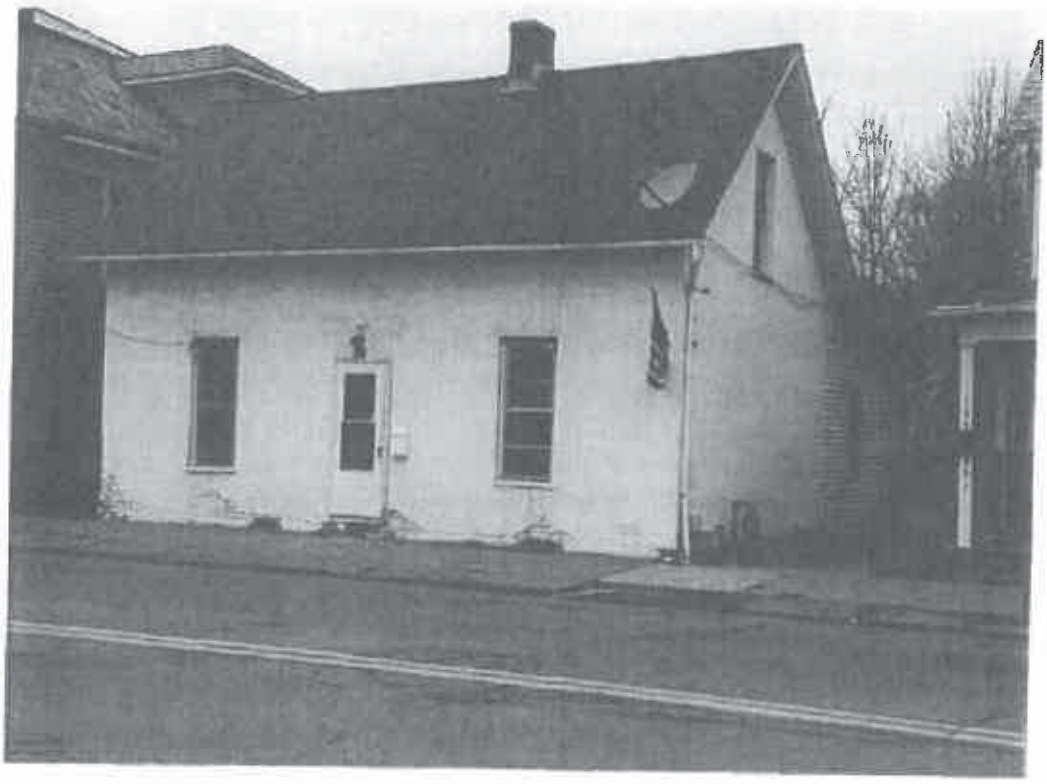
United States Magistrate Judge
United States District Court
Southern District of Ohio

ATTACHMENT A

DESCRIPTION OF PLACE TO BE SEARCHED

The place to be searched is the residence described below, including all its appurtenances, parking areas, outdoor working areas, detached buildings, individuals at the residence who may be in possession of a mobile computing device, and any computing related devices or digital media located therein or thereon.

59 W. 6th Avenue Lancaster, OH 43130 is described as nine hundred square foot, one and a half story single family home with white stucco exterior and white front storm door. The numbers "159" are affixed above the front door.



ATTACHMENT B

LIST OF ITEMS TO BE SEIZED

The following materials which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252, and 2252A: the advertising of/for, distribution, receipt and possession of child pornography.

1. Computer(s), computer hardware (including but not limited to central processing units; internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives, diskettes, and other memory storage devices), computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files, web cache information and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography.
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of the computer, or by other means for the purpose of distributing or receiving child pornography.

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by U.S. mail or by computer, any child pornography.
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography, or the existence of sites on the Internet that contain child pornography or that cater to whose with an interest in child pornography.
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.
9. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
10. Any and all files, documents, records, or correspondence, in any format or medium (including, but not limited to, network, system, security, and user logs, databases, software registrations, data and meta data), that concern user attribution information.
11. Any and all cameras, film, videotapes or other photographic equipment.
12. Any and all visual depictions of minors, whether clothed or not, for comparison to and identification of any child pornography images or videos discovered.
13. Any and all address books, mailing lists, supplier lists, mailing address labels, and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child pornography or any visual depictions.

14. Any and all documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to occupancy or ownership of the premises described above, including, but not limited to, rental or lease agreements, mortgage documents, rental or lease payments, utility and telephone bills, mail envelopes, or addressed correspondence.
15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct.